PREVEIL

Choosing Between PreVeil and GCC High: A Business Guide for Defense Contractors

Executive Summary

DEFENSE CONTRACTORS dealing with Controlled Unclassified Information (CUI) are required to communicate and store CUI according to strict rules defined by NIST 800-171, CMMC, and the cyber incident reporting requirements outlined in DFARS 7012. Traditional cloud services, such as Commercial Microsoft 365, Google's Gmail and Drive, and Box are not compliant with these regulations.

The two most popular compliant choices are PreVeil (used in conjunction with Commercial Microsoft 365 or Gmail) and Microsoft's Government Cloud Computing High (GCCH) system. The right choice depends on your organization's size, business mix, collaboration needs, available resources, and compliance timeline. This guide examines each of these factors to help you make an informed decision.

1. Organization Size and Structure

Large Organizations (500+ Employees)

Large organizations, especially those who use the full suite of Microsoft product offerings and need all employees to be within the CMMC compliance boundary, will prefer GCCH. While it lacks some of the features of the Commercial offering, large organizations may desire Active Directory integration and the document management controls associated with Microsoft Purview Information Protection. GCCH is significantly more expensive than Microsoft's Commercial product offering, and a migration to GCCH can be complex and time consuming, but large organizations often have the budget and project management expertise to support their preference for a "100% Microsoft" deployment.

Small and Medium Organizations (Under 500 Employees)

For small and medium-sized businesses, PreVeil typically provides the most practical path to compliance. These organizations benefit from PreVeil's significantly lower costs (license costs for PreVeil + Microsoft Office Suite are typically 40% less than GCC High) and simpler deployment model. The ability to overlay PreVeil on existing systems rather than performing a complete infrastructure migration proves especially valuable for organizations with limited IT resources and budget constraints.

Teams and Divisions Within Large Organizations

When only specific teams or divisions handle CUI, creating an enclave with PreVeil often makes more business sense than deploying GCC High across the entire organization. This approach allows organizations to maintain their existing IT infrastructure for non-CUI operations while ensuring compliance where needed. The selective deployment model can result in substantial cost savings and minimal business disruption.

2. Business Mix

Exclusively Defense

Companies with the entirety of their business dealing with CUI may prefer GCCH. In this case, all company emails and files will be managed by GCCH. The significantly higher cost may be worth it for an organization preferring to have all data treated as CUI.

Mix of Defense and Commercial

Companies balancing both defense and commercial businesses will prefer PreVeil because PreVeil easily enables you to create an "enclave" for dealing with CUI, whereas GCCH is designed to communicate primarily with other GCCH tenants. While it is possible to create an enclave using GCCH, it requires separate CUI and non-CUI email addresses for each user & complex management. Compare that to PreVeil, where a company can standardize on Commercial Microsoft 365 for all employees and just deploy PreVeil to those who deal with CUI. Here's how it works: PreVeil email integrates with Microsoft Outlook to create mailboxes for CUI. These mailboxes keep CUI encrypted on PreVeil servers and preserve the "regular" non-encrypted mail on Commercial servers — without requiring the encrypted email to use a special email address.

3. Third-Party Collaboration Requirements

Organizations That Can Mandate Technology Choices

Because GCCH is designed to connect primarily with other GCCH systems, it may be attractive for contractors who can require their third parties to also use GCC High. While it's possible to purchase additional GCC High licenses for customers and suppliers, this approach requires significant in-house IT resources to set up and manage external access, increases licensing costs, and creates ongoing administrative overhead.

Organizations That Need Flexible Collaboration

PreVeil proves most valuable for contractors who need to share CUI with customers and suppliers without forcing technology choices upon them. Third parties can access CUI through the PreVeil Express portal at no cost, with no software installation or downloads required. The web-based application enables secure sharing of both email messages and files while allowing third parties to manage their own PreVeil usage independently. This self-service approach eliminates administrative burden, accelerates partner onboarding, and maintains security without requiring partners to change their existing systems or purchase new licenses.

4. Compliance & IT Resources

Organizations with Significant IT Resources

Companies with dedicated IT teams, significant compliance expertise, and the ability to manage complex system migrations may be well-positioned to implement GCC High. These organizations can handle the extensive planning, documentation, and training required for a successful GCC High deployment. The platform's complexity demands continuous attention from IT staff for maintenance and updates.

Organizations with Constrained IT Resources

To be sure, becoming compliant is no easy task no matter which system is chosen. But PreVeil offers the Compliance Accelerator, a set of videos and pre-filled CMMC documentation that simplifies and accelerates the compliance journey. PreVeil's network of independent consultants and assessors are familiar with the PreVeil system and its associated compliant configurations. That knowledge can save significant time and expense compared with those who have to create customized plans from scratch.

5. Compliance Timeline

Organizations with Extended Timelines

GCC High implementations require six months to a year for full deployment. The process demands extensive planning and assessment before beginning a complex system migration. Organizations must also simultaneously manage CMMC control implementation and develop extensive custom

compliance documentation. This multi-layered approach creates significant schedule risk and usually requires substantial external consulting support.

Organizations with More Immediate Compliance Needs

PreVeil deployments can be completed in days or weeks by overlaying existing systems, rather than replacing them. Initial setup takes 1-2 days, with full deployment achieved in 2-4 weeks. Users are up-and-running quickly since PreVeil integrates with familiar tools like Outlook, Gmail, and File Explorer. PreVeil also accelerates compliance with pre-filled documentation and 1x1 videos to walk you through the 110 controls. As Jonathan Kelley, VP of Operations at Select Group – which achieved CMMC compliance with a perfect 110 score – explains:

> **"When it comes to speed to compliance and cost, PreVeil is undoubtedly the right decision. We got it done on time and on budget, saving $200,000 compared to GCC High. GCC High is a huge system implementation PLUS you have to meet 110 controls PLUS do all the documentation – so if you care about being on time, GCC High is a much bigger risk than PreVeil."**

6. Security Requirements

Organizations Maintaining Legacy Security

GCC High relies on traditional perimeter-based defenses and standard Microsoft security protocols. It offers optional enhanced encryption that uses central key servers, password-based authentication, and standard admin controls where administrators maintain full access to organizational data. While this traditional approach may be familiar, it creates potential vulnerabilities through password theft, central points of attack, and exposure to phishing attempts.

Organizations Requiring Best-in-Class Security

PreVeil implements modern Zero Trust security principles as recommended by the NSA. Its end-to-end encryption ensures data is only decrypted on end-user devices, eliminating vulnerable central points of attack. The platform's key-based authentication removes password risks, while distributed admin trust prevents single-admin compromise. Through Trusted Communities features, organizations can restrict communication to pre-approved domains and addresses, effectively preventing phishing and spoofing attacks.

Making the Final Decision

THE CHOICE BETWEEN PREVEIL AND GCC HIGH ultimately depends on your organization's specific circumstances. Consider these key factors:

- Organization Size and Structure
- Business Mix
- Third-Party Collaboration
- Compliance & IT Resources
- Compliance Timeline
- Security Requirements

GCC High may be the better choice for large defense contractors, where all employees handle CUI, where partners can be required to use the same system, where substantial IT and compliance resources are available, and where organizations are comfortable with legacy security and can accommodate a lengthy implementation timeline.

PreVeil typically serves as the optimal solution for small and medium sized businesses, or enclaves within larger companies, where customers and suppliers can use their own IT systems of choice, where best-in-class security is preferred, and where the cost and speed of compliance are paramount.

Appendix

How PreVeil Saves 75% vs. Microsoft GCC High and Offers Highest Security Level

	PREVEIL	MICROSOFT GCC HIGH
PRODUCT	**Email and File Sharing**	**Email and File Sharing**
COST	Low cost. PreVeil licenses are significantly more affordable than GCC High, and fewer licenses are needed, since you can limit to only users that access CUI. This results in a typical customer saving 75% vs GCC High.	High cost and complex. Upgrading to GCC High involves extensive planning, new infrastructure, business disruption, and higher license fees. Typically deployed across entire organization.
DEPLOYMENT	Integrates seamlessly with existing IT environments without rip and replace, saving time and money. No impact to existing file servers and users keep their regular email address.	Expensive and time-consuming rip and replace of file server and domain. Difficult to integrate with higher education's diverse computing environments, leading to compatibility issues and fragmented communication across the organization.
THIRD-PARTY COLLABORATION	Third parties can create free PreVeil accounts, enabling secure communication within minutes.	Cannot communicate with users outside of GCC High. Instead, expensive and difficult-to-manage guest licenses are required, adding admin burdens on IT team.
COMPLIANCE DOCUMENTATION SUPPORT	Save tens of thousands of dollars with pre-filled documentation including a System Security Plan, Standard Operating Procedures, POAM templates & more. Plus, C3PAO-validated videos and 1×1 support from our compliance team if you get stuck.	Institutions must develop their own documentation—a time-consuming and costly challenge given the complex configuration of the system.
MAINTENANCE	Simplified maintenance. Fewer software patches mean less time spent on maintenance and updating compliance documentation.	Frequent patches and updates required place significant burden on IT teams and divert their time from other critical tasks.
SECURITY		
ZERO TRUST	Built on Zero Trust principles as recommended by NSA.	Relies on legacy perimeter-based defenses.
ENCRYPTION	End-to-end encryption. No one but the intended recipient—including PreVeil—can ever read users' messages and files.	Optional enhanced encryption uses a key server, creating a vulnerable central point of attack.
AUTHENTICATION	Key-based authentication that eliminates passwords. Keys can't be guessed or stolen.	Uses passwords, increasing vulnerability to password theft and brute-force attacks.
ADMIN PROTECTION	Admin Approval Groups ensure that no single admin can compromise the enterprise	Administrators have full access to all data, creating a security risk
TRUSTED LISTS	Trusted Communities feature restricts communication to pre-specified domains and email addresses.	N/A—users' email exposed to untrusted phishing and spoofing attacks.